



Homeland Security

Cyber Security Research and Development (CSRD)

Broad Agency Announcement 04-17

(BAA04-17)

Proposer Information Pamphlet (PIP)

Department of Homeland Security

**Homeland Security Advanced Research Projects Agency
(HSARPA)**

September 9, 2004

For Questions Regarding This Solicitation:

BAA04-17@dhs.gov



Table of Contents

1	BACKGROUND	1
2	PROGRAM OBJECTIVES	1
2.1	Category 1: System Security Engineering	2
2.2	Category 2: Security of Operational Systems	5
2.3	Category 3: Investigative and Prevention Technologies	7
3	PROGRAM APPROACH	9
3.1	Program Structure	9
3.2	Government Furnished Equipment and Resources	10
3.3	Review Panel	10
3.4	Test and Evaluation Facilities	10
4	DELIVERABLES	11
4.1	Technical and Management Deliverables	11
4.1.1	Monthly Reports	11
4.1.2	Quarterly Reports	12
4.1.3	Annual Reports	12
4.2	Additional Deliverables	12
5	INFORMATION FOR OFFERORS	12
5.1	Eligible Applicants	12
5.2	Organizational Conflict of Interest	13
5.3	Anticipated Funding Level	13
5.4	Types of Awards Including Other Transactions for Prototypes	13
5.5	BAA Information	13
5.6	Submitting a Response to this BAA	14
5.6.1	Proprietary Protection	14
5.7	Bidders Conference	14
5.8	Security	14
5.9	Solicitation and Awards Schedule	15
5.10	White Paper Guidance and Content	15
5.10.1	White Paper Organization	16
5.11	Full Proposal Guidance and Content	17
5.11.1	Volume I, Technical and Management Proposal	17
5.11.2	Volume II, Cost Proposal	19
5.12	Contact Information	20
5.13	Objections to Solicitation and Award	21
6	EVALUATION CRITERIA AND SELECTION PROCESS	22
6.1	White Papers	22

6.1.1	Technical Approach	22
6.1.2	Performance Goals.....	22
6.1.3	Commercialization Capabilities and Plan	22
6.1.4	Personnel and Performer Qualifications and Experience	22
6.1.5	Costs, Work and Schedule	22
6.2	Proposals	22
6.2.1	Technical Approach.....	23
6.2.2	Performance Goals.....	23
6.2.3	Commercialization Capabilities and Plan	23
6.2.4	Personnel and Performer Qualifications and Experience	23
6.2.5	Cost Realism	23
6.3	Review and Selection Process	23
7	LIST OF ATTACHMENTS	24

1 BACKGROUND

The Science and Technology (S&T) Directorate in the Department of Homeland Security (DHS) has the mission to conduct research, development, test and evaluation (RDT&E) and timely transition of cyber security capabilities to operational units within DHS, as well as federal, state, local and critical infrastructure sector operational end-users for homeland security purposes. Cyber security is defined in broad terms to encompass the usual attributes of security as well as reliability, availability, and survivability in the face of adversary attack and accidental fault, while preserving privacy.

The Homeland Security Advanced Research Projects Agency (HSARPA) invests in programs offering the potential for revolutionary changes in technologies that promote homeland security and accelerate the prototyping and deployment of technologies that reduce homeland vulnerabilities. HSARPA performs these functions in part by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public or private entities, businesses, federally funded research and development centers and universities. The Department of Homeland Security (DHS) bears the responsibility of helping to secure a substantial portion of our Nation's Critical Infrastructure (including information and telecommunications, transportation, postal and shipping, emergency services and government continuity) but it does not own or control this infrastructure (which according to estimates is 85% owned and operated by the private sector).

2 PROGRAM OBJECTIVES

Cyber attacks are increasing in frequency and impact. Although to date there has not been a cyber attack that has had a significant impact on our Nation's critical infrastructures these attacks have demonstrated that there are extensive vulnerabilities in information systems and networks, with the potential for serious damage. The effects of a successful cyber attack might include serious economic consequences in terms of the impact to major economic and industrial sectors, threats to infrastructure elements such as electric power, and results that impede the response and communications capabilities of first responders in crisis situations.

A critical area of focus for DHS is the development and deployment of technologies to protect the nation's cyber infrastructure including the Internet and other critical infrastructures that depend on computer systems for their mission. The goals of the Cyber Security Research and Development (CSRD) program are:

- To perform research and development (R&D) aimed at improving the security of existing deployed technologies and to ensure the security of new emerging systems;
- To develop new and enhanced technologies for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure.

- To facilitate the transfer of these technologies into the national infrastructure as a matter of urgency.

To achieve these goals, this BAA calls for research and development in three categories with seven Technical Topic Areas (TTAs). The first category (TTAs 1-3) is concerned with tools and methodologies for developing secure systems, the second category (TTAs 4-5) addresses security of operational systems, and the third category (TTAs 6-7) focuses on a specific DHS customer need. Proposals shall be submitted to one of the seven TTAs and shall be structured to be one of three Type classifications depending on the maturity of the technology. A description of each of the Type classifications (I-New Technologies, II-Prototype Technologies, and III-Mature Technologies) is provided in section 3.1.

The criteria for determining the success of the proposed efforts should be explicitly defined in the proposals, with the expectation that projects will be judged on these criteria throughout their lifetimes. Such criteria might address the relative effectiveness of the proposed approaches, demonstrations of their usefulness in real systems, and the extent to which these approaches are adopted elsewhere (for example). These criteria should be associated with project milestones on an annual basis, to identify the benefits that would emerge in the event a project is not funded to completion.

2.1 Category 1: System Security Engineering

The first set of technical topic areas (TTAs 1-3) address the tools and methodological advances needed for the creation of more secure systems. The goal of category 1 of the CSRD Program is to develop and deploy capabilities that ensure the security of the cyber infrastructure before these systems leave the development laboratory for deployment in the field, and technologies that can be used in the analysis of operational systems and networks.

Identified Category 1 TTAs are:

TTA 1 - Vulnerability Prevention.

Today's computer systems and software are susceptible to a wide range of attacks. Better methods and tools are needed to significantly reduce or eliminate vulnerabilities, in existing systems and networks, as well as in newly emerging ones.

This topic area solicits practical approaches to:

- Development of software with improved security, reliability, and survivability architecturally built in, to minimize the number of vulnerabilities;
- Methods and tools for security requirements capture and analysis;
- Security architecture design and analysis for legacy systems and new systems;

- Implementation guidelines for secure software; methods for identifying well-known and more subtle flaws in specifications and implementations for systems and networking software;
- Test and evaluation of software with stringent security requirements;
- Better criteria for evaluation; maintenance and evolution of secure software; and
- Approaches that dramatically improve operational and administrative control and security policy management.

The emphasis should be primarily on making effective use of what is known from past research and development efforts, rather than exploring completely new paradigms. However, within that context innovation and novel approaches are clearly desirable.

TTA 2 - Vulnerability Discovery and Remediation.

Latent vulnerabilities are a certainty even in the best engineered systems. Methods and tools for identifying, analyzing and rectifying latent vulnerabilities are needed. For a number of reasons, not all software used in networked environments will be developed to a high level of assurance. Given the interconnected nature of networked systems, the community needs tools and techniques to identify, analyze the impact of, and remediate vulnerabilities.

TTA 2 seeks to encourage research and development of tools and techniques for analyzing software to detect security vulnerabilities. Techniques that require access to source code, as well as binary-only techniques, are in scope for this TTA. Specific goals for these tools and techniques should include (but are not limited to) providing solutions for the following:

- Buffer overflow detection/prevention;
- Other memory corruption problems (e.g., pointer use errors);
- Race conditions;
- Improper API use that results in vulnerabilities;
- Other flaws in security models or implementation, rather than simply bugs or programming errors;
- Script Injection;
- Insecure credential handling;
- Credential checking.

Recent work in software model-checking shows promising results in achieving the stated goals. Other techniques, e.g., metacompilation, are also applicable. New forms of static analysis are encouraged, as well as new runtime monitoring techniques. Innovative combinations of these techniques are strongly encouraged, to synergize the benefits of each, while minimizing the difficulties.

There are two obvious ways to measure the effectiveness of these tools: (1) Run them against large code bases (e.g., a Linux kernel, a FreeBSD release, KDE, etc.) and see how many existing vulnerabilities are found, as well as how many new vulnerabilities are found; or (2) benchmark new tools against analysis results for common programs that have been studied and analyzed in the literature, and for which a body of vulnerabilities is known (e.g., sendmail, Apache, WU-FTPD, etc.).

TTA 3 - Cyber Security Assessment.

The goal of this technical topic area is to develop methods and tools for assessing the cyber security of information systems. Assessing these systems is a costly and labor-intensive exercise which is largely ad hoc today (with the exception of a few highly trusted systems). The end result of this lack of system assessment capability is that systems are routinely deployed without a coherent understanding of their cyber security characteristics or a set of management guidelines for maintaining an adequate security posture. TTA 3 seeks research ideas that can remedy this situation.

Specific objectives include (but are not limited to):

- **Cyber Security Measurement:** Metrics that can be used to understand how well a system is meeting its security requirements. For example, resistance to attacks could be such a metric which would be related to the level of effort required of a specific class of attacker to break a system. Other metrics might relate to the continuity of mission that the system is supporting. These metrics can be used to add consistency to the assessment process.
- **Cyber Security Analysis:** Practical and scalable methods that show analytically that certain security properties are met. Such methods must be easily accessible and usable by the people that build software and hardware systems.
- **Benchmarks:** Microprocessors are marketed using benchmarks, as opposed to conclusive proofs that they will perform in certain ways for all possible applications. Benchmarks capture the essence of the most important problems a system is likely to be called upon to address and thus allow comparisons between different systems. There is no such capability for comparing systems in terms of their security properties. Research is needed to define sets of typical cyber security properties and scenarios, backed up by solid metrics, to allow such comparisons to take place.
- **Information Security Cases:** Security assessment must not merely result in a single number — a one-dimensional metric cannot possibly capture the range of properties or aspects that need to be assessed. This has long been recognized in safety critical systems where assessment is multidimensional and captures both process and product elements in a safety case - a reasoned coherent argument that supplies evidence to support the system designer claims. Research is needed to define appropriate argument structures in the case of information security, and to create supporting tools to aid the construction and maintenance of information security cases.

2.2 Category 2: Security of Operational Systems

Efforts to develop software and systems that are more secure will take time to pay dividends, and even in the best case the national information infrastructure will remain vulnerable to serious attack for some time. It is not clear that any of the current stakeholders – developers, service providers, user communities, and so on – have the national infrastructure perspective in mind. DHS seeks technologies that protect the national critical information infrastructure, and that specifically address issues that may not be at the forefront for the commercial sector. The goals of Category 2 of the CSRD Program are to develop and deploy secure capabilities for existing systems, and to ensure the operational security of these systems in the field.

Identified Category 2 TTAs are:

TTA 4 - Security and Trustworthiness for Critical Infrastructure Protection (CIP)

The Nation's critical infrastructures are seriously at risk from a wide range of very significant potential threats. All of these infrastructures are increasingly dependent on computers and communications. Consequently, the threats to the existing cyber infrastructures are themselves threats to the national infrastructures. This is inherently undesirable, and must be corrected over time through the use of system-oriented approaches that address all relevant risks. Both short-term and long-term remedies are needed, with strategies for providing increasing measures of security within the proposed time frame.

General purpose computers are increasingly being used for mission-critical tasks within critical infrastructures. Moreover, these systems are increasingly integrated into enterprise networks. These trends permit companies to leverage advances in commercial technology and more closely integrate business and production activities. Adoption of these technologies has allowed for great improvements in efficiency, safety, and response to market forces. However, there is concern that this has come at the price of increasing the vulnerability of these systems to network attack. The mission-critical function of these systems is availability, and it has often been the case that concerns of security are not given due weight. In particular, it is conjectured that security technologies, such as security patches, are not diligently applied to such systems.

This TTA seeks to encourage research and development of tools and technologies to improve the security posture of current critical infrastructure systems. The tools and technologies should be focused in the following areas: 1) automated security vulnerability assessments for critical infrastructure systems (as there is current reluctance to apply these tools due to the impact of the assessment itself and the very stringent availability requirements of such systems); 2) improvements in system robustness of critical infrastructure systems and associated commercial service providers to operate through network attacks, even if the attack impacts enterprise systems closely connected with the specific critical infrastructure systems; 3) configuration and security policy

management to ensure proper operations and access of critical infrastructure systems; and 4) large-scale cross-platform and/or cross network attack correlation and aggregation, both among individual infrastructure areas and across different infrastructure sectors.

Criteria for success should be explicitly defined in the proposals, and must address specific demonstrations of improvements over what exists today. In particular, these criteria must address security issues such as system and network integrity, early detection and timely prevention of large scale attacks to whatever extent possible, and survivability of the critical infrastructures in the large in the presence of a stated range of potential adversities focused on but not entirely constrained to cyber attacks.

TTA 5 - Wireless Security. With the explosive growth in the adoption of Wireless Fidelity (WiFi) networking in recent years, the limitations of wireless security have become a topic of widespread concern. Given little if any ability to restrict unauthorized traffic through the ether, and an uncertain array of security models, security-related communication protocols, and related encryption protocols that have not achieved consistent usage, or worse have failed to ensure their claimed security requirements, the interest in WiFi security solutions is well founded. This technical topic area explores the significant security challenges that arise in the deployment of public and private WiFi networks, and seeks new dynamic solutions to recognize and mitigate WiFi security threats.

Dynamic control of basic service set networks: DHS seeks innovative technical solutions that will provide the foundation for new security services, authentication, and access control mechanisms in computer-based WiFi networks. This performance area focuses on the development of technologies to facilitate the analysis of WiFi asset communications for the purposes of dynamically adjusting security posture, authentication services, and group membership rights. Offerors are encouraged to submit proposals focused on, but not limited to, the following topic areas:

- New commodity hardware to facilitate advanced analysis services, to include multi-channel communications, RF Signal interference and signal diagnosis, and software interfaces;
- High-fidelity solutions for WiFi signal location in closed structures
- Integration of location-based access control;
- Methods for advanced signal fingerprinting analysis, synthetic flow communication detection;
- Solutions for rogue client and access point interception and active forensics.

Ad-hoc network security research: The future of non-fixed infrastructure WiFi networking will rely heavily on cooperative mobile ad-hoc networks. This performance area seeks innovative solutions to self-securing wireless network device services and cooperative security protection services. Offerors are encouraged to submit proposals regarding

- Agent-based dynamic coordination access control in ad-hoc network membership
- Non-centralized threat analysis of global and propagating attacks in ad-hoc network infrastructures
- Behavior-based analysis and dynamic exclusion of WiFi assets

2.3 Category 3: Investigative and Prevention Technologies

The last set of technical topic areas (TTAs 6 & 7) address several of the tools and methodological advances needed for technologies to assist industry and law enforcement communities in responding to hostile cyber threats. The goal of category 3 of the CSRD Program is to develop and deploy capabilities that can ensure the security of the cyber infrastructure, in general, and assist some critical infrastructure sectors as they work with law enforcement to better defend their sectors.

Identified Category 3 TTAs are:

TTA 6 - Network Attack Forensics.

Today's networks continue to be the target of attack. Insider misuse is an important special case of this problem. This TTA is focused on the development of methods and tools for traceback and identification of network attackers.

The traceback problem can be broken down into two research areas. The first research area is the problem of tracing the path of a datagram through the Internet, the so-called "IP Traceback" problem. So far, we have seen three primary classes of schemes in this area: (a) "Bloom filters" that require state in the routes, (b) Probabilistic Packet Marking (PPM) schemes, and (c) algebraic packet marking. More research, especially simulations and pilot projects, is needed in IP traceback to produce efficiently deployable solutions.

The second major traceback research area can be called "attack traceback." In a typical distributed denial of service (DDoS) attack, a master computer controls a number of zombie computers. IP traceback, described above, can discover the location of the zombie computers, but generally not the master computer. The problem in attack traceback is to discover the master computer. Typical approaches to this problem include forms of traffic analysis and correlation. Attack traceback schemes need to be robust in the face of encrypted traffic between masters and zombies.

This TTA seeks to encourage research and development of tools and techniques for both areas of the traceback problem. Refinements to existing traceback methods, as well as innovative new proposals, are solicited in both areas of traceback. Specific goals for these tools and techniques should include (but are not limited to):

- IP traceback against a large number of zombies (e.g., 100,000) deployable in the real world

- Attack traceback in the Internet with realistic assumptions

Many approaches to IP traceback have been proposed in the literature. All of these provide basic building blocks for research in this TTA. While innovative new techniques are in scope, the primary focus should be on moving these technologies towards wide scale deployment. While the literature on attack traceback is much thinner, the documented discussion of traffic analysis provides a starting point.

Metrics for this TTA in IP traceback include storage requirements, computational requirements, number of zombies that can be distinguished, and number of packets required for successful traceback. For attack traceback, the metrics should consider the number of streams of attack traffic, and the amount of noise (e.g., other traffic) in the network.

TTA 7 - Technologies to Defend against Identity Theft

Technology and the rapid growth of the Internet have eliminated the traditional borders of financial crimes and provided new opportunities for those who engage in fraud to threaten the nation's financial systems. New technologies have been exploited by an expanding criminal element that conducts a host of sophisticated financial crimes. Telecommunications and finance systems may become prime targets for organized crime or potentially cyber-terrorists intent on causing damage to the economy of the United States. DHS elements and their law enforcement partners at the federal, state and local levels, work closely with members of telecommunications and finance industries and the academic community to share information and identify weaknesses.

Identity crime involves the theft or misuse of personal or financial identifiers in order to gain something of value and/or facilitate other criminal activity. The different types of identity crime include identity theft, credit card/access device fraud, check fraud, bank fraud, false identification fraud and passport/visa fraud. Identity crime is important to investigate because it involves multiple victims, usually has a large dollar loss, is often used by organized criminal groups, and is usually associated with other crimes such as drugs/narcotics, mail theft/fraud, electronic crime and terrorism. The concern that money obtained in large-scale identity crimes could be used to finance terrorist activity places the fight against such crimes on the homeland security agenda. A particular form of identity crime that is increasing at an alarming rate is "phishing", a class of high-tech scam that uses fraudulent e-mail to deceive consumers into visiting fake replicas of familiar Web sites and disclosing their credit card numbers, bank account information, Social Security numbers, passwords and other sensitive information.

This TTA seeks to encourage research and development of tools and techniques for defending against identity theft and other financial systems attacks. For anti-phishing technologies to be deployed on desktops, we must keep in mind that the target user base is not the expert user community. Instead, solutions must work for all types of users, most importantly for the less sophisticated users who are the ones most likely to fall for

phishing scams. Any technology that requires end-users to change their behavior will face hard challenges. It will be very important to scientifically evaluate the usability of any technology that end-users will be exposed to. Any solution must be easily integrated into existing information infrastructure, for example, Web browsers and servers, e-mail clients and gateways, Internet service provider infrastructure, and security products and services.

3 PROGRAM APPROACH

3.1 Program Structure

Proposals shall be structured in phases per one of the three Type classifications described below, depending on the maturity of the proposed technology. The deployment phase shall outline the test, evaluation and deployment of the technology, and shall be included as an option in the proposal for Type I and II technologies.

Type I (New Technologies): proposals requesting funding for new technologies shall have an applied research phase, a development phase, and a deployment phase, with the emphasis on development and deployment. Proposals may request funding for a timeframe not to exceed 36 months (including the deployment phase).

Type II (Prototype Technologies): proposals requesting funding for more mature prototype technologies shall have a development phase and a deployment phase. Proposals may request funding for a timeframe not to exceed 24 months (including the deployment phase).

Type III (Mature Technologies): proposals requesting funding for a mature technology shall have a deployment phase only. Proposals may request funding for a timeframe not to exceed 12 months.

The objective of this structure is to support immediate technology transition wherever possible and create transition paths for new capabilities from the outset. Proposers must also include a description in the proposal of their plan for commercializing the technology or otherwise get the technology into established transition paths, such as the open source community. This request does not entail providing a full business plan, nor does it imply that DHS views commercialization activities as being within the scope of this solicitation. The intent is for offerors to provide evidence that as part of the technical plan development, consideration has been given to the ultimate commercialization of the outputs of DHS-funded programs including expected user base, how the technology will be used, and how it would get into broad use. Of key importance are the identification of technology diffusion path(s) that are appropriate for the type and maturity of the technology involved, and any additional factors that might increase the likelihood of it being commercialized. Proposals will be evaluated with other proposals that are submitted to the same TTA (1-7) and have the same Type (I-III) classification.

3.2 Government Furnished Equipment and Resources

Transition ready technologies provided by DHS strategic partner laboratories may be included as GFE through the procedure outlined in Appendix A of the BAA. HSARPA neither encourages nor discourages bidders from incorporating DHS strategic partner laboratory technologies. The inclusion of these technologies is at the sole discretion of HSARPA bidders in their evaluation of best value and best technical response to the government under this solicitation. Teams should identify any requested strategic partner laboratory GFE as part of their proposals, including all costs associated with the inclusion of the GFE.

In addition, the Government will consider requests from teams submitting Type I and Type II proposals for Government furnished equipment (GFE) and resources. Type III proposals are not eligible for GFE. Teams should identify any requested GFE as part of their proposals.

3.3 Review Panel

A review panel drawn from Government and non-Government experts who have signed appropriate non-disclosure agreements will perform a technical evaluation of the proposals as outlined in section 6. Bidders may request a government only review, but must indicate so when submitting on the website.

3.4 Test and Evaluation Facilities

Performers in the CSRD technical program will be required to test and evaluate their technologies with respect to system performance goals and may use the facilities of the Cyber Defense Technology Experimental Research (DETER) network and/or other facilities as appropriate. The DETER testbed will provide the necessary infrastructure — networks, tools, and supporting processes — to support national-scale experimentation on emerging security research and advanced development technologies.

The DETER testbed and the associated Evaluation Methods for Internet Security Technologies (EMIST) research projects are jointly funded by HSARPA and the National Science Foundation (NSF). The project objectives are to build an effective experimental and testing environment and to develop a corresponding experimental methodology for Internet security issues and defense mechanisms.

The centerpiece of the experimental environment is a safe (quarantined) but realistic network testbed. The design of the DETER testbed is based upon a mesh of clusters of homogeneous experimental nodes. Each cluster is based upon Utah's Emulab hardware and software, with additions and modifications to provide the security and isolation that is a unique requirement of the DETER testbed. Following NSF's recommendation that network research testbeds should be driven by the needs and goals of networking

researchers, the DETER testbed is being designed to meet the particular needs of researchers in network security. Important examples of application areas for the DETER testbed are DDoS defense, worm propagation and defense, and defense of the network control plane, e.g., routing infrastructure and domain name system (DNS). In addition to the testbed itself, the DETER and EMIST projects are creating a supporting software environment of attack, defense, traffic generation, measurement, and analysis tools.

Bidders to the CSRD technical program should bear in mind that the design of the DETER testbed is itself an important research and engineering problem, and that they should not expect a ready-made “turnkey” platform on which their proposed technologies can be immediately tested and evaluated. Rather, CSRD performers should expect to become active participants in the community of security researchers that will shape the development of the DETER testbed. Accordingly, bidders should consider the specific test and evaluation requirements of their proposed technical solutions and include plans (and associated budgets) for their participation in the DETER community. Bidders may also propose alternative test and evaluation plans, showing clearly how the proposed alternative will better serve the CSRD program with respect to system performance goals.

More information on the DETER testbed design, implementation, and operational policies and procedures can be found at the main DETER project Web site at <http://www.isi.edu/deter/> and the testbed operations Web site at <http://www.isi.deterlab.net/>.

4 DELIVERABLES

To the exclusion of exceptions negotiated at time of award, any of the deliverables associated with this Program may be released to outside organizations, both U. S. Government and non-Government, in support of DHS S&T efforts. The performer may recommend a preferred format for each deliverable, but the Government will determine the final format.

4.1 Technical and Management Deliverables

4.1.1 Monthly Reports

Brief (not more than one page) narrative reports will be electronically submitted to the Program Manager within one week after the last day of each month. These reports will describe the previous 30 calendar days’ activity, technical progress achieved against goals, difficulties encountered, recovery plans (if needed), and explicit plans for the next 30 day period. A separate financial report that outlines the expenditures over the same time period will also be provided.

4.1.2 Quarterly Reports

Quarterly reports (not to exceed 5 pages) will be electronically submitted to the Program Manager and are due one week prior to the time of the quarterly reviews. These reports will describe the previous 90 calendar days' activity, principals involved in the actual work of the period, technical progress achieved against goals, difficulties encountered, funds expended against each sub-task in the previous 90 day period, recovery plans (if needed), and explicit plans for the next 90 day period. A separate financial report that outlines the expenditures over the same time period will also be provided.

4.1.3 Annual Reports

At the end of each full year of performance, a full report will be delivered to the Program Manager that describes the achievements of the project, the current work of the project, and the outlook for progress in the subsequent year. This report should contain a full accounting of how the awarded funds were spent.

4.2 Additional Deliverables

Performers should define additional concept and program specific deliverables as appropriate for their specific proposal.

5 INFORMATION FOR OFFERORS

5.1 Eligible Applicants

Any entity or team of entities, other than the specific Department of Energy Laboratories listed in Appendix A, may submit a white paper and/or proposal in accordance with the requirements and procedures identified in this Broad Agency Announcement (BAA). Historically Black Colleges and Universities (HBCU), Minority Institutions (MI), Small and Disadvantaged Businesses (SDB), Women-owned Businesses (WB), and HUB-zone enterprises are encouraged to submit proposals, and to join others in submitting proposals; however, no portion of the BAA will be set-aside for these special entities because of the impracticality of reserving discrete or severable areas of research and development under this topic.

Teams, which may include private sector organizations, Government laboratories including Federally Funded Research and Development Centers (FFRDCs), and academic institutions, are encouraged to respond.

5.2 Organizational Conflict of Interest

Organizational Conflict of Interest issues will be evaluated on a case by case basis as outlined in Appendix B. Offerors who have existing contract(s) to provide Scientific, Engineering, Technical and/or Administrative support directly to the program officers or other operational activities of the Science and Technology Directorate will receive particular scrutiny.

5.3 Anticipated Funding Level

HSARPA anticipates that up to \$4.5 M in funding will be available for multiple awards under the Cyber Security R&D solicitation. Refer to section 3.1 for additional information on the required structure for the proposal.

5.4 Types of Awards Including Other Transactions for Prototypes

Awards may be executed as contracts, grants, cooperative agreements or other transactions. Section 831(a)(2) of the Homeland Security Act of 2002 (Public Law 107-296) gives the Department of Homeland Security (DHS) the same “Other Transactions for Prototypes” authority exercised by the Department of Defense (DoD) under 10 U.S.C. §2371 note. Section 831(a)(2) also imposes the same criteria for award of an “Other Transactions for Prototypes” agreement on DHS as was given to DoD.

5.5 BAA Information

Copies of this BAA may be downloaded from the FedBizOpps web site at www.FedBizOpps.gov or at www.hsarpabaa.com. Paper copies of the BAA may be obtained by contacting:

Booz Allen Hamilton,
4001 Fairfax Drive, Suite 750
Arlington, VA 22203
POC: Steve Svensson 703-465-2628

Booz Allen Hamilton is a support contractor for HSARPA and as such is excluded from participating as a bidder in this or any other non-support HSARPA procurement.

5.6 Submitting a Response to this BAA

White papers and proposals will be submitted electronically using the HSARPA BAA Web Site: www.hsarpabaa.com. To aid in the management of this solicitation, bidders are required to register in advance to submit a proposal. Bidders will not be permitted to electronically submit proposals unless registered. The registration deadline is listed in Table 1 of section 5.9. Proposals will be disqualified if registration is not completed by the deadline. Instructions for registration can be found at www.hsarpabaa.com. Upon registration or submission, a file will be sent to the registered email address. Receipt of a file confirms your registration or proposal submission. Please check the contents of the file. If they are incorrect, return to the website and make corrections.

While the submission of a white paper is not a requirement to submitting a proposal, potential offerors are STRONGLY urged to avail themselves of the white paper process.

5.6.1 Proprietary Protection

All data uploaded to HSARPA BAA Web Site is protected from public view or download. All submissions will be considered proprietary/source selection sensitive and protected accordingly. Documents may only be reviewed by the registrant, authorized Government representatives, and assigned evaluators.

5.7 Bidders Conference

HSARPA will hold a Bidders Conference for the CSRD BAA on September 23rd at the Hilton Crystal City in Arlington, Virginia. All interested attendees must register on line at <https://www.enstg.com/signup/passthru.cfm?ConferenceCode=DHS26146> or linking from www.hsarpabaa.com. A \$145.00 registration fee will be collected at sign in. The point of contact for the Bidders Conference is:

Donna Blanger
Booz-Allen Hamilton
703-807-2795
blanger_donna@bah.com.

5.8 Security

No classified bids are expected or desired. There is no mechanism for the submission of classified proposals. There is no requirement for personnel working on this effort to have or obtain security clearances.

5.9 Solicitation and Awards Schedule

DATE	EVENT
9 September 2004	BAA published in FedBizOps
23 September 2004	Bidder's Conference
27 September 2004	White Paper Registration Deadline
6 October 2004	White Papers due @ 4PM EDT
3 November 2004	White Paper Feedback Provided to Bidders
17 November 2004	Full Proposal Registration Deadline
1 December 2004	Proposals due @ 4:00PM EST
18 January 2005	Awards Announced

Table 1 - Procurement Schedule

5.10 White Paper Guidance and Content

Offerors are strongly encouraged, but not required, to submit white papers in advance of full proposals.

White papers should capture the essence of a proposal and are designed to permit offerors to obtain feedback from HSARPA on their planned technology development without having to go to the expense and effort of writing a complete proposal. A white paper may consist of not more than five pages including all pictures, figures, tables, and charts in a legible size.

If received by the white paper submission deadline, the white paper will be evaluated by a review panel. After this review, offerors will be promptly notified either encouraging submission of a full proposal or discouraging submission of a complete proposal.

A white paper is PDF file format (minimum 12 point font size and not less than single line spacing), readable by IBM-compatible PCs. The individual file size must be no more than 5 Mb.

The white paper should contain the following information in the following order:

- Executive Summary
- Technical Approach
- Personnel and Performer Qualifications and Experience
- Commercialization Capabilities
- Costs, Work and Schedule

5.10.1 White Paper Organization

Adherence to the following organization will expedite review of the white papers.

5.10.1.1 *Executive Summary*

Provide a concise description of the scientific, technical, engineering and management approach you propose to address the TTA. Describe the various features of the proposed technology and relevant details about how it will achieve the goals of the TTA. Point out what is unique about your proposed solution.

5.10.1.2 *Technical Approach*

Describe the basic scientific or technical concepts that comprise your proposed solution to the problem described in the TTA. Explain what is unique about your solution and what advantages it might afford compared to other approaches that have been taken in this area. Illustrate the particular scientific, technical and/or engineering issues that need to be addressed and resolved to demonstrate feasibility.

5.10.1.3 *Personnel and Performer Qualifications and Experience*

Briefly describe the offeror's qualifications and experience in similar development efforts. Present the qualifications of the principal technical team leaders. Describe the extent of your team's past experience in working with or developing the technologies comprising your solution.

5.10.1.4 *Commercialization Capabilities and Plan*

Provide a brief summary of the offeror's capabilities and experience in transitioning similar products to the marketplace, including previous business partnerships that can be leveraged. Describe the commercialization plan or other transition method for getting the technology into wide-spread use.

5.10.1.5 *Costs, Work and Schedule*

Provide a brief summary of the planned work, costs, and schedule required to execute your project, summarized by task. Describe all required material, such as, previously developed technology, wireless networks or test facilities, which must be provided by the Government to support the proposed work.

5.11 Full Proposal Guidance and Content

Bidders will be able to initiate Proposal Registration at www.hsarpabaa.com only after the deadline for White Paper feedback provided in Table 1 of section 5.9. Following Proposal Registration, bidders may begin submitting proposals which must be submitted prior to the proposal deadline. Although white papers are strongly encouraged, bidders may submit a proposal without a preceding white paper.

Offerors can choose to alter their ideas, concepts, technical approaches, etc. or expand on their original ideas between submission of a white paper and submission of the full proposal. Discussion, suggestions, or advice between the Government and offerors on white paper topics is not binding. Offerors are free to submit a full proposal without regard to any feedback or advice about white papers that they may have received. Even if the feedback from the Government in response to the white paper is that a proposal based on the offered idea is unlikely to receive funding, a full proposal may still be submitted and will be evaluated uniformly with others.

Proposals consist of two separate electronic documents described in detail below. The first electronic file contains all technical information and is titled *Volume I, Technical and Management Proposal*. The second electronic document displays all cost information and is titled *Volume II, Cost Proposal*.

The two volume proposal is written in PDF file format (minimum 12 point font size and not less than single line spacing) for IBM-compatible format or, if more convenient for Volume II, Microsoft Excel. *Volume I, Technical and Management Proposal* shall not exceed forty (40) pages. There is no page limit on *Volume II*. The forty page limitation for Volume I includes all pictures, figures, tables, and charts in a legible size. Maximum file size is 5 Mb. Responsiveness to the order and content of sections listed in Volume I is important to assure thorough and fair evaluation of proposals. The submission of other supporting materials with the proposal is strongly discouraged and if submitted, will not be reviewed. Nonconforming proposals may be rejected without review.

5.11.1 Volume I, Technical and Management Proposal

5.11.1.1 Official Transmittal Letter

This is an official transmittal letter with authorizing official signature. For electronic submission, the letter can be scanned into the electronic proposal. The letter of transmittal shall state whether this proposal has been submitted to another government agency, other than HSARPA, and if so, will specify which agency and when it was submitted.

5.11.1.2 *Executive Summary*

This is a one page synopsis of the entire proposal including total costs. This page should include the proposal title and company name. Provide a description of the scientific, technical, engineering and management approach you propose to address the goals of the TTA. Point out what is unique about your proposed solution. Include a brief summary of your technology's anticipated performance relative to the TTA goals.

This section shall be separable, i.e., it will begin on a new page and the following section shall begin on a new page.

5.11.1.3 *Proposal*

This section describes the proposed work and the associated technical and management issues.

- a. **Performance goals:** Describe the overall methodology and how it will meet the goals specified in the TTA.
- b. **Detailed technical approach (no more than 15 pages):** Describe the proposed design and technical issues. Identify the critical technical issues in the design and concept.
- c. **Statement of Work (SOW), Schedule and Milestones:** Provide an integrated display for the proposed research, showing each task with major milestones. Include a section clearly marked as the Statement of Work you propose to undertake.
- d. **Deliverables:** Provide a brief summary of all deliverables proposed under this effort, including data, software and reports consistent with the objectives of the work involved.
- e. **Management Plan:** Provide a brief summary of the management plan, including an explicit description of what role each participant or team member will play in the project, and their past experience in technical areas related to this Proposal.
- f. **Commercialization Plan:** Describe, in general terms, the company's capabilities and experience in transitioning similar products to the marketplace (including previous business partnerships that can be leveraged) and specific plans for diffusion of technology developed via work proposed under this program. For Type I proposals provide the company's strategy in taking the proposed technology from government sponsored research and development to commercialization. For Type II proposals provide the company's strategy in taking the prototype technology from development to commercialization. For Type III proposals provide the company's strategy for commercialization of the technology and/or plan for getting the technology into wide-spread use, e.g., insertion into open source distribution channels.
- g. **Facilities:** List the location(s) where the work will be performed and the facilities to be used. Describe any specialized or unique facilities which bear directly on the effort.

- h. **Government Furnished Resources:** Provide a brief summary of required information and data which must be provided by the Government to support the proposed work, if any.
- i. **Cost Summary:** Summarize the projected total costs for each task in each year of the effort including a summary of subcontracts, man hours, and consumables.
- j. **Resumes for key personnel:** In Appendix A provide resumes and curriculum vitas (CVs) for each of the key personnel.
- k. **Other DHS support:** As an appendix provide a list of any current or pending awards and/or proposals with DHS. (This section will not count toward the 40 page limit).

5.11.2 Volume II, Cost Proposal

The Cost Proposal will include:

5.11.2.1 Cost Response

The cost response should be in the offeror's format. Detailed Bases of Estimates are not required. Certified cost or pricing data are not required. However, in order for the government to determine the reasonableness, realism and completeness of the cost proposal, the following data must be provided for the principal investigator and each team member and in a cumulative summary:

- **Labor:** Total labor includes direct labor and all indirect expenses associated with labor, to be used. Labor hours shall be allocated to each work outline element and segmented by team member. A labor summary by work outline is required. Provide a breakdown of labor and rates for each category of personnel to be used on this project.
- **Direct Materials:** Total direct material that will be acquired and/or consumed. Limit this information to only major items of material and how the estimated expense was derived. For this agreement, a major item exceeds \$10,000. Material costs shall be assigned to specific work outline elements.
- **Subcontracts:** Describe major efforts to be subcontracted, the source, estimated cost and the basis for this estimate. For this agreement a major effort exceeds \$250,000. Subcontract labor and material shall be accounted for per the two paragraphs above. A summary chart showing each major subcontractor labor and material effort by work outline is required.
- **Travel:** Total proposed travel expenditures. Limit this information to the number of trips, location, duration, and purpose of each trip.
- **Other Costs:** Any direct costs not included above. List the item, the estimated cost, and basis for the estimate.

The Cost Proposal should be consistent with your proposed SOW. Activities such as demonstrations required to reduce the various technical risks should be identified in the SOW and reflected in the Cost Proposal. The offeror should provide a total estimated

price for the major IR&D activities associated with the program. The offeror should state whether each program is dedicated IR&D or if it is being pursued to benefit other programs as well.

5.11.2.2 *Cost Share*

Cost sharing is not required. Teams proposing cost share should identify the amount, timing, and source(s) of funds and provide the supporting rationale for cost sharing. Costs shared by the team shall be allocated to each relevant work outlined in the proposal.

5.11.2.3 *Award Mechanisms*

Awards may be issued as a FAR contract, Other Transaction for Research, Other Transaction for Prototype, cooperative agreement or grant. Bidders may request a specific award mechanism. Teams requesting a non-FAR based award must submit the rationale for their selection. Information on Other Transaction Authority is given in Appendix D. The final selection of award mechanism will be made by the Government.

5.12 Contact Information

The applicable electronic address for all correspondence for this BAA is: BAA04-17@dhs.gov. To ensure proper logging and prompt response to questions about this BAA, potential submitters are encouraged to use this email address for all correspondence.

HSARPA Program Manager:

Dr. Douglas Maughan

Homeland Security Advanced Research Projects Agency

Washington, D.C. 20407

202-254-6145

douglas.maughan@dhs.gov

Contracting Officer Technical Representatives (COTR)/Contracting Officer Representatives (COR)*:

Kevin Kumferman (COTR)

SPAWAR Systems Center - San Diego (SSC-SD)

Code 24121

53560 Hull Street

San Diego, CA 92152-5001

Phone: 619-553-0851

Fax: 619-553-1690

kevin.kumferman@navy.mil

Gloria Golden (COR)

DOI/NBC

P.O. Box 12924
Fort Huachuca, AZ 85670-1292
Phone: 520 538-0418
Fax: 520-533-1600
gloria_m_golden@nbc.gov

Robert Kaminski (COTR)
AFRL/IFG
525 Brook Road
Rome, NY 13441-4505
Phone: 315-330-1865
Fax: 315- 330-1894
Robert.Kaminski@rl.af.mil

Cliff Wang, PhD (COTR)
Computing and Information Science Division
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211
Phone: 919-549-4207
Fax: 919- 549 - 4248
cliff.wang@us.army.mil

*Contact the COTR for any technical questions, and contact the COR for any contracting questions

5.13 Objections to Solicitation and Award

Any objections to the terms of this solicitation or to the conduct of receipt, evaluation or award of agreements must be presented in writing within ten calendar days of (1) the release of this solicitation or (2) the date the objector knows or should have known the basis for its objection. Objections should be provided in letter format, clearly stating that it is an objection to this solicitation or to the conduct of the evaluation or award of an agreement, and providing a clearly detailed factual statement of the basis for objection. Failure to comply with these directions is a basis for summary dismissal of the objection. Mail objections to the address listed in the proposal delivery information.

6 EVALUATION CRITERIA AND SELECTION PROCESS

6.1 White Papers

White papers will be evaluated with other white papers that are submitted to the same TTA number (1-7) and are of the same Type classification (I-III). The evaluation of the white papers will be accomplished through an independent technical review of each using the following criteria:

6.1.1 Technical Approach

Sound technical and managerial approach to the proposed work, including a demonstrated understanding of the critical technical or engineering challenges required for achieving the goals of the TTA.

6.1.2 Performance Goals

Potential of the proposed technology/solution for meeting the goals of the TTA.

6.1.3 Commercialization Capabilities and Plan

Assessment of the commercialization experience and strategy to determine the likelihood that the offeror will be able to deploy a technology and/or solution that can be transitioned effectively to the user community either through commercialization of the technology or through other means.

6.1.4 Personnel and Performer Qualifications and Experience

Capability of the team to perform the proposed work, and the history of performance of the principal investigator and the team members in developing related technologies.

6.1.5 Costs, Work and Schedule

Assessment of the realism of the proposed costs, work to be performed, and schedule.

6.2 Proposals

Awards will be made based on the evaluation, funds availability, and other programmatic considerations. The Government reserves the right to fund none, some, parts, or all of the proposals received. Proposals will be evaluated with other proposals that are submitted to the same TTA number (1-7) and are of the same Type classification (I-III). The evaluation of proposals shall be accomplished through an independent review of each

proposal using the following criteria, which are listed in descending order of relative importance:

6.2.1 Technical Approach

Sound technical and managerial approach to the proposed work, including a demonstrated understanding of the critical technical or engineering challenges required for achieving the goals of the TTA.

6.2.2 Performance Goals

Potential of the proposed technology/solution for meeting the goals of the TTA.

6.2.3 Commercialization Capabilities and Plan

Assessment of the commercialization experience and strategy to determine the likelihood that the offeror will be able to deploy a technology and/or solution that can be transitioned effectively to the user community either through commercialization of the technology or through other means. Evaluation of the commercialization plan or other transition method and the likelihood that the proposed technology/solution will be successfully transitioned to the user community.

6.2.4 Personnel and Performer Qualifications and Experience

Capability to perform proposed work, and history of performance of the team in developing related technologies.

6.2.5 Cost Realism

The Government will independently assess whether the cost is appropriate. Cost realism is only used as an evaluation criterion in cases where the cost is not reasonable for the proposed effort

.

6.3 Review and Selection Process

It is the policy of HSARPA to ensure an impartial, equitable, and comprehensive evaluation of all white papers and proposals and to select the source, or combination of sources, whose offer is most advantageous for the Government. In order to provide the desired evaluation, Government employees and contractors will review each submission. These personnel will have signed, and will be subject to, the terms and conditions of non-disclosure agreements. Bidders may request a government-only review, but must indicate so during the white paper and/or proposal registration at <http://www.hsarpabaa.com>.

Notwithstanding a request for a government-only review, the Government intends to use employees and contractors to assist in administering the evaluation of white papers and proposals. These personnel will have signed, and will be subject to, the terms and conditions of non-disclosure agreements.

7 LIST OF ATTACHMENTS

Appendix A List of Excluded Bidders

Appendix B Organizational Conflict of Interest

Appendix C List of Acronyms

Appendix D OTA Rules

Appendix A: List of Excluded Bidders

The Department of Energy Laboratories listed below, termed DHS strategic partner laboratories, are not permitted to propose as the lead or prime contractor under this solicitation, nor may they be included on any team except under the very limited circumstances of providing transition ready technologies as described in detail below.

- 1) Argonne National Laboratory (ANL)
- 2) Brookhaven National Laboratory (BNL)
- 3) DoE Remote Sensing Laboratory (RSL)
- 4) Idaho National Environmental and Engineering Laboratory (INEEL)
- 5) Lawrence Livermore National Laboratory (LLNL)
- 6) Los Alamos National Laboratory (LANL)
- 7) Oak Ridge National Laboratory (ORNL)
- 8) Pacific Northwest National Laboratory (PNNL)
- 9) Sandia National Laboratory (SNL).

The DHS strategic partner laboratories may only participate in this solicitation by supporting eligible bidders subject to the following rules:

- 1) DHS strategic partner laboratories may not propose directly to this solicitation or participate in any manner in the development of responses to this solicitation outside of the process here defined.
- 2) The DHS strategic partner laboratories may collaborate with HSARPA bidders by providing explicitly identified transition ready technologies subject to DOE and DHS approval. It is on the initiative of the providing laboratory to identify which technologies are transition ready.
- 3) In addition to transition ready technologies, the DHS strategic partner laboratories may collaborate with HSARPA bidders by providing explicitly identified and unique supporting capabilities subject to DOE and DHS approval. It is on the initiative of the providing laboratory to identify which supporting capabilities are available to HSARPA bidders.
- 4) HSARPA will neither encourage nor discourage bidders from incorporating DHS strategic partner laboratory technologies. The inclusion of these technologies is at the sole discretion of HSARPA bidders in their evaluation of best value and best technical response to the government under this solicitation.
- 5) All collaborations between HSARPA bidders and performers and DHS strategic partner laboratories is subject to any additional restrictions imposed by either the collaborating laboratory or the DOE.

The process for DHS strategic partner laboratories to participate in this HSARPA solicitation is defined below:

- 1) The DHS strategic partner laboratories, at their initiative, will propose a list of transition ready technologies or unique supporting capabilities. This list is subject to the approval of DHS (ORD & HSARPA). Once approved, this list is published at www.hsarpabaa.com with supporting technical documentation.
- 2) HSARPA bidders may request the addition of technologies not listed as part of this BAA. This request must be submitted to HSARPA and is subject to the approvals identified above.
- 3) White papers and proposals which include ineligible laboratory participation outside of this process will be rejected without review.
- 4) For the purposes of the white paper submission, HSARPA bidders may identify as part of their technical solution any of the published transition ready technologies or unique supporting technologies without laboratory, DHS or DOE consultation or approval. (Step 1)
- 5) Based upon the number of inquiries and other factors, individual DHS strategic partner laboratories may elect not to provide additional technical data beyond the public technical disclosures at the white paper stage. (Step 1)
- 6) White papers will be evaluated assuming the requested technologies will be made available to the bidder.
- 7) The DHS strategic partner laboratory POC is responsible to ensure that technical discussions with the HSARPA bidders are limited to the technologies and capabilities published in conjunction with this BAA and must explicitly ensure that no discussions involve any internal DHS data provided to the DHS strategic partner laboratories.
- 8) Prior to submission of a full proposal, HSARPA bidders must negotiate a statement of work including costs with the appropriate DHS strategic partner laboratory which must be submitted as part of the full proposal. This negotiation is subject to all normal laboratory and DOE policies with regard to collaboration and technology transition. (Step 2)
- 9) Selected proposals which include DHS strategic partner laboratory participation are subject to final approval of the HSARPA Director with regards to the level of effort and scope of the DHS strategic partner laboratory participation. (Step 3)
- 10) Selected proposals may be subject to final negotiation of any technology transfer or collaborative agreements needed to implement the proposed work. (Step 3)

Solicitation Steps

Step 1: Submission of White Papers

- No discussions with DHS strategic partner laboratories required or guaranteed

Step 2: Submission of Full Proposals

- Limited discussion with DHS strategic partner laboratory POC
- Collaboration on DHS strategic partner laboratory Statement of Work

Step 3: Selection of Proposals

- Discussions/negotiations between bidder and DHS strategic partner laboratory POC

Step 4: Award of Contracts

Appendix B: Organizational Conflict of Interest

ORGANIZATIONAL CONFLICT OF INTEREST

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to mitigate or avoid such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

(1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

(2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included the mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation/Waiver. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes it can be mitigated, neutralized, or avoided, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan. If not defined, then this provision applies fully.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestitures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

Appendix C: Acronym List

BAA – Broad Agency Announcement
CSRD – Cyber Security Research and Development
CIP – Critical Infrastructure Protection
COR – Contracting Officer Representative
COTR – Contracting Officer Technical Representative
DHS – Department of Homeland Security
DDoS – Distributed Denial of Service
DETER – Cyber Defense Technology Experimental Research
DNS – Domain Name Server
DoD – Department of Defense
DoE – Department of Energy
EDT – Eastern Daylight Time
EST – Eastern Standard Time
EMIST – Evaluation Methods for Internet Security Technologies
FAR – Federal Acquisition Regulations
FedBizOps – Federal Business Opportunities (www.FedBizOps.gov)
FFRDC – Federally Funded Research and Development Centers
GFE – Government Furnished Equipment
HBCU – Historically Black Colleges and Universities
HSARPA – Homeland Security Advanced Research Projects Agency
HUB – Historically Underutilized Business
IP – Internet Protocol
IR&D – Independent Research and Development
MI – Minority Institutions
NSF – National Science Foundation
OTA – Other Transaction Agreement
PDF – Portable Document Format
PIP – Proposal Information Pamphlet
R&D – Research and Development
RDT&E – Research, Development, Test and Evaluation

S&T – Science and Technology

SBIR – Small Business Innovative Research

SDB – Small and Disadvantaged Businesses

SOW – Statement of Work

TTA – Technical Topic Area

WB – Women-owned Businesses

Appendix D: Model Other Transaction (OT) Agreement

Section 831(a)(2) of the Homeland Security Act of 2002 (Public Law 107-296) gives the Department of Homeland Security (DHS) the same “Other Transactions for Prototypes” authority exercised by the Department of Defense (DoD) under 10 U.S.C. §2371 note. Section 831(a)(2) also imposes the same criteria for award of an “Other Transactions for Prototypes” agreement on DHS as was given to DoD.

In summary, these criteria require that:

- 1) there must be either at least one nontraditional government contractor participating to a significant extent in the prototype project; or,
- 2) if there is no nontraditional government contractor participating to a significant extent, at least one of the following circumstances exists:
 - i) at least one third of the total cost of the prototype project is to be paid with funds provided by parties to the transaction other than the Federal Government; or,
 - ii) the senior procurement executive determines that exceptional circumstances justify the use of a transaction that provides for innovative business arrangements or structures that would not be feasible or appropriate under a contract.

In this context, a “nontraditional contractor” is defined as:

- 1) an entity that has not, for a period of at least one year prior to the date that a transaction (other than a contract, grant, or cooperative agreement) for a prototype project under the authority of this section is entered into, entered into or performed with respect to –
 - i) any contract that is subject to full coverage under the cost accounting standards prescribed pursuant to section 26 of the Office of Federal Procurement Policy Act (41 U.S.C. 422) and the regulations implementing such section; or
 - ii) any other contract in excess of \$500,000 to carry out prototype projects or to perform basic, applied, or advanced research projects for a Federal agency, that is subject to the Federal Acquisition Regulation.

The Government has discretion in determining the level of “significant extent.” Some factors may include:

- 1) criticality of the technology being contributed

- 2) role of the non-traditional government contractor(s) in the design process
- 3) value of the effort being proposed

Contributions for items such as IR&D reimbursement, G&A, cost of money, and fee identified separately will meet the statutory cost-share requirement and are preferred to in-kind contributions. It is not the Government's intention to encourage or require use of the cost share criteria. The Government prefers that the teams attempt to locate appropriate non-traditional team members before offering cost share. If the team cannot or chooses not to find nontraditional team members or provide cost share, the team may request a waiver of these requirements. The team should describe the innovative business arrangements or structures that would justify the exercise of such a waiver. The Government will consider all waiver requests but reserves the right to grant any, all or none of the requests at its discretion.

MODEL OTHER TRANSACTION (OT) AGREEMENT - *NOTE: HSARPA is willing to negotiate terms and conditions in the Offeror's proposed agreement prior to receipt of the proposal. This negotiation may begin immediately upon receipt of proposed agreement.*

OTHER TRANSACTION FOR PROTOTYPE MODEL AGREEMENT

BETWEEN (INSERT TEAM NAME AND ADDRESS)

AND

THE HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY
7TH & D ST., SW
WASHINGTON, DC 20528

CONCERNING:

CYBER SECURITY RESEARCH AND DEVELOPMENT

Agreement No.: *(Insert agreement number)*

HSARPA Order No.:

Total Estimated Government Funding of the Agreement: \$

Team's Cost Share/Contribution: \$

Funds Obligated: \$

Authority: Section 831 of the Homeland Security Act of 2002, Public Law 107-296

Line of Appropriation: AA

This Agreement is entered into between the United States of America, hereinafter called the Government, represented by The Homeland Security Advanced Research Projects Agency (HSARPA), and the (INSERT NAME of TEAM) pursuant to and under U.S. Federal law.

FOR (INSERT TEAM NAME)

FOR THE UNITED STATES OF
AMERICA

(Signature)
(Name, Title)

(Date)

(Signature)
(Name, Title)

(Date)

TABLE OF CONTENTS

ARTICLES

ARTICLE I	Scope of the Agreement
ARTICLE II	Term
ARTICLE III	Statement of Objectives
ARTICLE IV	Payable Event Schedule and Deliverables
ARTICLE V	Agreement Administration
ARTICLE VI	Obligation and Payment
ARTICLE VII	Disputes
ARTICLE VIII	Patent Rights
ARTICLE IX	Data Rights
ARTICLE X	Foreign Access to Technology
ARTICLE XI	Civil Rights Act
ARTICLE XII	Government Furnished Property
ARTICLE XIII	Security
ARTICLE XIV	Optional Future Phases
ARTICLE XV	Order of Precedence
ARTICLE XVI	Entire Agreement

ATTACHMENTS

ATTACHMENT 1	Statement of Work
ATTACHMENT 2	Integrated Master Schedule

ARTICLE I: SCOPE OF THE AGREEMENT

This article should state your vision for the HSARPA Cyber Security Research and Development Program and describe how your proposed project satisfies the statement of objectives. Be sure to discuss the commercial uses of the developed technologies.

In addition, this article should discuss the way you will interact with the HSARPA program team. Suggested wording (i.e., paragraphs used in other HSARPA Agreements) for your consideration follows:

“HSARPA will have continuous involvement with the Contractor. HSARPA will obtain access to program results and certain rights to patents and data pursuant to Articles VIII and IX. HSARPA and the Contractor are bound to each other by a duty of good faith and best effort in achieving the program objectives.”

“This Agreement is an ‘other transaction’ pursuant to Section 831 of the Homeland Security Act of 2002, Public Law 107-296. The Parties agree that the purpose of this Agreement is to acquire the Team's best efforts in development of design concepts and trade-off studies supporting that design. The delivery of this design is a prototype within the meaning of the above-mentioned statute. The Federal Acquisition Regulation (FAR) applies only as specifically referenced herein. This Agreement is not intended to be, nor shall it be construed as, by implication or otherwise, a partnership, a corporation, or other business organization.”

Terms such as “Team,” “Team Members” and “program,” etc. should also be defined in this article.

ARTICLE II: TERM

A. The Term of this Agreement

This Agreement commences upon the date of the last signature hereon and continues for the duration of the Cyber Security Research and Development Program. For planning purposes, the estimated period of performance is date of award through 24 months. Completion criteria are defined in Article IV, Payable Event Schedule and Deliverables.

B. Termination Provisions

Subject to a reasonable determination that this agreement will not produce beneficial results commensurate with the expenditure of resources, either Party may terminate this Agreement by written notice to the other Party, provided that such written notice is preceded by consultation between the Parties. In the event of a termination of the Agreement, it is agreed that disposition of data developed under this Agreement, shall be in accordance with the provisions set forth in Articles IX, Data Rights. The Government and Team will negotiate in good faith a reasonable and timely adjustment of all

outstanding issues between the Parties as a result of termination. Failure of the Parties to agree to a reasonable adjustment will be resolved pursuant to Article VII, Disputes. The Government has no obligation to reimburse the Team beyond the last completed and paid milestone if the Team decides to terminate.

C. Extending the Term

The Parties may extend by mutual written agreement the term of this Agreement if funding availability and research opportunities reasonably warrant. Any extension shall be formalized through modification of the Agreement by the Agreements Officer and the Team Administrator.

ARTICLE III: STATEMENT OF OBJECTIVES

This article should also summarize the scope of the work and the business arrangement to which you are committing (as described in detail in this article, Statement of Objectives) by entering into this Agreement.

The Team will include here or reference here their proposed Statement of Work (SOW) in accordance with the guidance provided in the solicitation. This SOW describes the tasks that the Team must accomplish to be successful.

ARTICLE IV: PAYABLE EVENT SCHEDULE AND DELIVERABLES

A. Payment Schedule

The Team shall perform the work required by Article III and the SOW. The Team shall be paid for each Payable Milestone accomplished and delivered in accordance with the Schedule of Payments and Payable Milestones set forth below. The Team shall propose the accomplishment criteria for the events listed below. Both the Schedule of Payments and the Funding Schedule set forth below may be revised or modified in accordance with subparagraph C of this article.

B. Schedule of Payments and Payable Milestones

C. Modifications

1. At any time during the term of the Agreement, progress or results may indicate that a change in the Statement of Objective and/or the Payable Milestones would be beneficial to the program objectives. Recommendations for modifications, including justifications to support any changes to the Statement of Objectives and/or the Payable Milestones, will be documented in a letter and submitted by the Team to the HSARPA Program Manager with a copy to the HSARPA Agreement Officer. This letter will detail the technical, chronological, and financial impact of the proposed modification to the research program. Any resultant modification is subject to mutual agreement of the parties. The

Government is not obligated to pay for additional or revised Payable Milestones until the Payable Milestones Schedule is formally revised by the HSARPA Agreements Officer and made part of this Agreement.

2. The HSARPA Program Manager shall be responsible for the review and verification of milestone accomplishment criteria and any recommendations to revise or otherwise modify the Agreement Statement of Objectives, Schedule of Payments and Payable Milestones, or other proposed changes to the terms and conditions of this Agreement.

3. For minor or administrative Agreement modifications (e.g., changes in the paying office or appropriation data, changes to Government or Team personnel identified in the Agreement, etc.), HSARPA shall make these types of changes unilaterally

4. The Government will be responsible for effecting all modifications to this agreement.

ARTICLE V: AGREEMENT ADMINISTRATION

Administrative and contractual matters under this Agreement shall be referred to the following representatives of the parties:

HSARPA: *(Name will be inserted)* Agreements Officer, Tel: *(Number will be inserted)*
Team: (INSERT NAME) (INSERT TITLE) (INSERT TELEPHONE NUMBER)

Technical matters under this Agreement shall be referred to the following representatives:

HSARPA: *(Name will be inserted)*, Program Manager, Tel: *(Number will be inserted)*
Team: (INSERT NAME) (INSERT TITLE) (INSERT TELEPHONE NUMBER)

Either party may change its representatives named in this Article by written notification to the other party. The Government will effect the change as stated in subparagraph C.4 of Article IV above.

ARTICLE VI: OBLIGATION AND PAYMENT

A. Obligation

The Government's liability to make payments to the Team is limited to only those funds obligated under this Agreement or by amendment to the Agreement. HSARPA may obligate funds to the Agreement incrementally.

B. Payments

1. The following information shall be included on each invoice:

Agreement Number
Invoice Number
A description of services performed
Quantity of service received or performed
The time of period covered by the invoice
Terms of Payment
Payment Office
Amount claimed

2. The Team shall document each Payable Milestone by submitting deliverables in accordance with the Payable Milestone Schedule and Accomplishment Criteria. The Team shall submit an original and one (1) copy of all invoices to the Agreements Officer for payment approval. After written verification of the accomplishment of the Payable Milestone by the HSARPA Program Manager, and approval by the Agreements Officer, the invoices will be forwarded to the payment office within fifteen (15) calendar days of receipt of the invoices at HSARPA. Payment approval for the final Payable Milestone will be made after reconciliation. Payments will be made by (*appropriate paying office will be inserted at time of award*) within fifteen (15) calendar days of HSARPA's transmittal. Subject to change only through written Agreement modification, payment shall be made via electronic funds transfer to the Contractor's address set forth below:

3. Bank Account of Payee:

Bank:
Address:
Routing Transit Number:
Depositor Account Title:
Depositor Number:

4. Financial Records and Reports: The Team's relevant financial records associated with this Agreement are not subject to examination or audit by the Government, except as noted below, since the confirmed accomplishment of the appropriate milestone completes the obligation of both parties.

5. Comptroller General Access to Records: To the extent that the total government payments under this Agreement exceed \$5,000,000, the Comptroller General, at its discretion, shall have access to and the right to examine records of any party to the agreement or any entity that participates in the performance of this agreement that directly pertain to and involve transactions relating to, the agreement for a period of three (3) years after final payment is made. This requirement shall not apply with respect to any party to this agreement or any entity that participates in the performance of the agreement, or any subordinate element of such party or entity, that has not entered into any other agreement (contract, grant, cooperative agreement, or "other transaction") that provides for audit access by a government entity in the year prior to the date of this agreement. This paragraph only applies to any record that is created or maintained in the

ordinary course of business or pursuant to a provision of law. The terms of this paragraph shall be included in all sub-agreements to the Agreement.

ARTICLE VII: DISPUTES

A. General

The Parties shall communicate with one another in good faith and in a timely and cooperative manner when raising issues under this Article.

B. Dispute Resolution Procedures

1. Any disagreement, claim or dispute between the Government and the Team concerning questions of fact or law arising from or in connection with this Agreement, and, whether or not involving an alleged breach of this Agreement, may only be raised under this Article.
2. Whenever disputes, disagreements, or misunderstandings arise, the Parties shall attempt to resolve the issue(s) involved by discussion and mutual agreement as soon as practicable. In no event shall a dispute, disagreement or misunderstanding which arose more than three (3) months prior to the notification made under subparagraph B.3 of this Article constitute the basis for relief under this article unless the Director of HSARPA in the interests of justice waives this requirement.
3. Failing resolution by mutual Agreement, the aggrieved Party shall document the dispute, disagreement, or misunderstanding by notifying the other Party (through the HSARPA Agreements Officer) in writing of the relevant facts, identify unresolved issues, and specify the clarification or remedy sought. Within five (5) working days after providing notice to the other Party, the aggrieved Party may, in writing, request a joint decision by the HSARPA Deputy Director, and Representative of the Team ("Team Representative"). The other Party shall submit a written position on the matter(s) in dispute within thirty (30) calendar days after being notified that a decision has been requested. The HSARPA Deputy Director and the Team Representative shall conduct a review of the matter(s) in dispute and render a decision in writing within thirty (30) calendar days of receipt of such written position. Any such joint decision is final and binding.
4. In the absence of a joint decision, upon written request to the Director of HSARPA, made within thirty (30) calendar days or upon unavailability of a joint decision under subparagraph B.3 above, the dispute shall be further reviewed. The Director of HSARPA may elect to conduct this review personally or through a designee or jointly with a representative of the other Party who is a senior official of the Party. Following the review, the Director of HSARPA or designee will resolve the issue(s) and notify the Parties in writing. Such resolution is not subject to further administrative review and, to the extent permitted by law, shall be final and binding.

ARTICLE VIII: PATENT RIGHTS

A. Definitions

1. “Invention” means any invention or discovery which is or may be patentable or otherwise protectable under Title 35 of the United States Code.
2. “Made” when used in relation to any invention means the conception or first actual reduction to practice of such invention.
3. “Practical application” means to manufacture, in the case of a composition of product; to practice, in the case of a process or method, or to operate, in the case of a machine or system; and, in each case, under such conditions as to establish that the invention is capable of being utilized and that its benefits are, to the extent permitted by law or Government regulations, available to the public on reasonable terms.
4. “Subject invention” means any invention of a Team Member conceived or first actually reduced to practice in the performance of work under this Agreement.

B. Allocation of Principal Rights

The Team shall retain the entire right, title, and interest throughout the world to each subject invention consistent with this Article and 35 U.S.C. § 202. With respect to any subject invention in which the Team retains title, HSARPA shall have a non-exclusive, nontransferable, irrevocable, paid-up license to practice or have practiced on behalf of the United States the subject invention throughout the world. Notwithstanding the above, the Team may elect to provide full or partial rights that it has retained to Team Members or other parties.

C. Action to Protect the Government's Interest

1. The Team agrees to execute or to have executed and promptly deliver to HSARPA all instruments necessary to (i) establish or confirm the rights the Government has throughout the world in those subject inventions to which the Consortium elects to retain title and to enable the Government to obtain patent protection throughout the world in that subject invention.
2. The Team shall include, within the specification of any United States patent application and any patent issuing thereon covering a subject invention, the following statement: “This invention was made with Government support under Agreement No. *(agreement number will be inserted at time of award)* awarded by HSARPA. The Government has certain rights in the invention.”

3. In order to insure world-wide interoperability of multiple vendor systems, the Government shall retain all rights to external interface standards, whether developed under this or similar programs, to include all communications protocols, data formats, encryption techniques and messaging protocols.

D. Lower Tier Agreements

The Team shall include this Article, suitably modified, to identify the Parties, in all subcontracts or lower tier agreements, regardless of tier, for experimental, development, or research work.

E. Reporting on Utilization of Subject Inventions

The Team agrees to submit a final report on the utilization of a subject invention or on efforts at obtaining such utilization that are being made by the Team or its licensees or assignees. The report shall include information regarding the status of development, date of first commercial sale or use, gross royalties received by the Team subcontractor(s), and such other data and information as the agency may reasonably specify. The Team also agrees to provide additional reports as may be requested by HSARPA in connection with any march-in proceedings undertaken by HSARPA in accordance with paragraph G of this Article. Consistent with 35 U.S.C. § 202(c)(5), HSARPA agrees it shall not disclose such information to persons outside the Government without permission of the Team.

F. Preference for American Industry

Notwithstanding any other provision of this Article, the Team agrees that it shall not grant to any person the exclusive right to use or sell any subject invention in the United States or Canada unless such person agrees that any product embodying the subject invention or produced through the use of the subject invention shall be manufactured substantially in the United States or Canada. However, in individual cases, the requirements for such an agreement may be waived by HSARPA upon a showing by the Team that reasonable but unsuccessful efforts have been made to grant licenses on similar terms to potential licensees that would be likely to manufacture substantially in the United States or that, under the circumstances, domestic manufacture is not commercially feasible.

G. March-in Rights

The Team agrees that, with respect to any subject invention in which it has retained title, HSARPA has the right to require the Team, an assignee, or exclusive licensee of a subject invention to grant a non-exclusive license to a responsible applicant or applicants, upon terms that are reasonable under the circumstances, and if the Team, assignee, or exclusive licensee refuses such a request, HSARPA has the right to grant such a license itself if HSARPA determines that:

1. Such action is necessary because the Team or assignee has not taken effective steps, consistent with the intent of this Agreement, to achieve practical application of the subject invention;
2. Such action is necessary to alleviate health or safety needs that are not reasonably satisfied by the Team, assignee, or their licensees;
3. Such action is necessary to meet requirements for public use and such requirements are not reasonably satisfied by the Team, assignee, or licensees; or
4. Such action is necessary because the agreement required by paragraph (I) of this Article has not been obtained or waived or because a licensee of the exclusive right to use or sell any subject invention in the United States is in breach of such Agreement.

ARTICLE IX: DATA RIGHTS

Government Purpose Rights in all data delivered under this agreement. The following standard Government Data Rights Article is offered as a point of departure in this case.

A. Definitions

1. “Government Purpose Rights”, as used in this article, means rights to use, duplicate, or disclose Data, in whole or in part and in any manner, for Government purposes only, and to have or permit others to do so for Government purposes only.
2. “Unlimited Rights”, as used in this article, means rights to use, duplicate, release, or disclose, Data in whole or in part, in any manner and for any purposes whatsoever, and to have or permit others to do so.
3. “Data”, as used in this article, means recorded information, regardless of form or method of recording, which includes but is not limited to, technical data, software, trade secrets, and mask works. The term does not include financial, administrative, cost, pricing or management information and does not include subject inventions included under Article VIII.
4. “Limited rights” as used in this article means the rights to use, modify, reproduce, release, perform, display, or disclose technical data, in whole or in part, within the Government. The Government may not, without the written permission of the party asserting limited rights, release or disclose the data outside the Government, use the technical data for manufacture, or authorize the technical data to be used by another party.

B. Allocation of Principal Rights

1. This Agreement is performed with mixed Government and Team funding. The Parties agree that in consideration for Government funding, the Team intends to reduce to practical application items, components and processes developed under this Agreement.

2. The Team agrees to retain and maintain in good condition until (INSERT NUMBER OF YEAR) (____) years after completion or termination of this Agreement, all Data necessary to achieve practical application. In the event of exercise of the Government's March-in Rights as set forth under Article VIII or subparagraph B.3 of this article, the Team, acting through its Team Lead, agrees, upon written request from the Government, to deliver at no additional cost to the Government, all Data necessary to achieve practical application within sixty (60) calendar days from the date of the written request. The Government shall retain Unlimited Rights, as defined in paragraph A above, to this delivered Data.

3. The Team agrees that, with respect to data necessary to achieve practical application, HSARPA has the right to require the Team to deliver all such data to HSARPA in accordance with its reasonable directions if HSARPA determines that:

(a) Such action is necessary because the Team or assignee has not taken effective steps, consistent with the intent of this Agreement, to achieve practical application of the technology developed during the performance of this Agreement;

(b) Such action is necessary to alleviate health or safety needs which are not reasonably satisfied by the Team, assignee, or their licensees; or

(c) Such action is necessary to meet requirements for public use and such requirements are not reasonably satisfied by the Team, assignee, or licensees.

4. With respect to data delivered pursuant to Attachment 3, Reports (and listed below), the Government shall receive Government Purpose Rights, as defined in paragraph A above. With respect to all Data delivered, in the event of the Government's exercise of its right under subparagraph B.2 of this article, the Government shall receive Unlimited Rights.

C. Marking of Data

Pursuant to paragraph B above, any data delivered under this Agreement shall be marked with the following legend:

“Use, duplication, or disclosure is subject to the restrictions as stated in Agreement (*appropriate agreement number will be inserted at time of award*) between the Government and the Team.”

D. Lower Tier Agreements

The Team shall include this Article, suitably modified to identify the Parties, in all subcontracts or lower tier agreements, regardless of tier, for experimental, developmental, or research work.

ARTICLE X: FOREIGN ACCESS TO TECHNOLOGY [Not Applicable]

ARTICLE XI: CIVIL RIGHTS ACT

This Agreement is subject to the requirements of Title VI of the Civil Rights Act of 1964 as amended (42 U.S.C. 2000-d) relating to nondiscrimination in employment.

ARTICLE XII: GOVERNMENT FURNISHED EQUIPMENT PROPERTY, INFORMATION FACILITIES AND SERVICES

The following Government Equipment property, information facilities, and services shall be provided upon the written approval of the cognizant contracting officers:

(Offeror will list all desired GFE, GFP, GFI, GFF, and GFS.)

ARTICLE XIII: SECURITY [Not Applicable]

ARTICLE XIV: OPTIONAL FUTURE PHASES [Not Applicable]

ARTICLE XV: ORDER OF PRECEDENCE

In the event of any inconsistency between the terms of this Agreement and its Attachments, the inconsistency shall be resolved by giving precedence in the following order: (1) the Agreement, (2) all other Attachments to the Agreement.

ARTICLE XVI: ENTIRE AGREEMENT

This Agreement constitutes the entire agreement of the Parties and supersedes all prior and contemporaneous agreements, understandings, negotiations and discussions among the Parties, whether oral or written, with respect to the subject matter hereof. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. This Agreement shall not be binding until the execution and delivery between each of the Parties of at least one set of counterparts.

ATTACHMENTS

- ATTACHMENT 1 STATEMENT OF WORK (SOW)
- ATTACHMENT 2 INTEGRATED MASTER SCHEDULE